Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently Amended) An apparatus for detecting adversarial activity on a network, comprising:

a memory adapted to store a host table;

a key exchanger adapted to repeatedly derive a cipher key such that the resulting cipher key changes over time;

a translator adapted to translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

a mapping device adapted to map the address to the host table;

a host resolution device adapted to issue a request to the network to resolve the address when the address does not match an entry in the host table and to supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and

an actuator adapted to trigger a security device when the address does not match an entry in the host table.

2. (Original) An apparatus as set forth in Claim 1, wherein the security device is a logging device adapted to log the data packet.

3. (Original) An apparatus as set forth in Claim 1, wherein the security device is adapted to signal an alarm when triggered.

4. (Previously Presented) An apparatus as set forth in Claim 1, wherein said host resolution device is adapted to derive the host table using an address resolution protocol.

5. (Original) An apparatus as set forth in Claim 1, further comprising:

a network device adapted to place the data packet onto a network when the address maps to the host table.

6. (Currently Amended) A method for detecting adversarial activity on a network, comprising:

storing a host table;

repeatedly deriving a cipher key such that the resulting cipher key changes over time;

translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

mapping the address to the host table;

issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and

triggering a security device when the address does not match an entry in the host table.

7. (Original) A method as set forth in Claim 6, further comprising:

logging the data packet when the address does not match an entry in the host table.

8. (Original) A method as set forth in Claim 6, further comprising:

signaling an alarm when the security device is triggered.

9. (Previously Presented) A method as set forth in Claim 6, further comprising: deriving the host table using an address resolution protocol.

10. (Original) A method as set forth in Claim 6, further comprising:

placing the data packet onto a network when the address maps to the host table.

11. (Currently Amended) A device for detecting adversarial activity on a network, comprising:

means for storing a host table;

means for repeatedly deriving a cipher key such that the resulting cipher key changes over time;

means for translating predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

means for mapping the address to the host table;

means for issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplementing the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and

means for triggering a security device when the address does not match an entry in the host table.

12. (Original) A device as set forth in Claim 11, further comprising:

means for logging the data packet when the address does not match an entry in the host table.

13. (Original) A device as set forth in Claim 11, further comprising:

means for signaling an alarm when the security device is triggered.

14. (Previously Presented) A device as set forth in Claim 11, further comprising: means for deriving the host table using an address resolution protocol.

15. (Original) A device as set forth in Claim 11, further comprising:

means for placing the data packet onto a network when the address maps to the host table.

16. (Currently Amended) A bastion host adapted for processing packet header information of a data packet, the bastion host being operable to:

store a host table;

repeatedly derive a cipher key such that the resulting cipher key changes over time;

translate predetermined portions of packet header information of a data packet according to a cipher algorithm keyed by the cipher key, wherein the predetermined portions include an address;

map the address to the host table;

issuing a request to the network to resolve the address when the address does not match an entry in the host table and supplement the host table with the address upon receipt of a reply to the request that indicates that the address is valid; and

trigger a security device when the address does not match an entry in the host table.

17. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to log the data packet when the address does not match an entry in the host table.

18. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to signal an alarm when the security device is triggered.

19. (Previously Presented) The bastion host as set forth in Claim 16, the bastion host being further operable to derive the host table using an address resolution protocol.

20. (Original) The bastion host as set forth in Claim 16, the bastion host being further operable to place the data packet onto a network when the address maps to the host table.

Claims 21 – 24 (Cancelled)

25. (New) An apparatus as set forth in Claim 1, wherein the address includes a network portion and an apparatus portion, and wherein said translator is adapted to translate the apparatus portion of the address without also translating the network portion of the address.

26. (New) An apparatus as set forth in Claim 1, wherein the data packet includes a header with a plurality of fields carrying packet header information, wherein said translator is adapted to translate at least a portion of the packet header information in one or more predetermined fields of the header into a translated packet header, the translated packet header including the translated packet header information in the one or more predetermined fields of the packet header interspersed with un-translated packet header information in fields other than the one or more fields of the packet header.

27. (New) A method as set forth in Claim 6, wherein the address includes a network portion and an apparatus portion, and wherein translating predetermined portions of packet header information includes translating the apparatus portion of the address without also translating the network portion of the address.

28. (New) A method as set forth in Claim 6, wherein the data packet includes a header with a plurality of fields carrying packet header information, wherein translating predetermined portions of packet header information comprises:

translating at least a portion of the packet header information in one or more predetermined fields of the header into a translated packet header, the translated packet header including the translated packet header information in the one or more predetermined fields of the

packet header interspersed with un-translated packet header information in fields other than the one or more fields of the packet header.

29. (New) A device as set forth in Claim 11, wherein the address includes a network portion and an apparatus portion, and wherein said means for translating predetermined portions of packet header information is adapted to translate the apparatus portion of the address without also translating the network portion of the address.

30. (New) A device as set forth in Claim 11, wherein the data packet includes a header with a plurality of fields carrying packet header information, wherein said means for translating predetermined portions of packet header information is adapted to translate at least a portion of the packet header information in one or more predetermined fields of the header, and is further adapted to copy the translated packet header information into the respective one or more fields of the header to thereby generate a translated packet header, the translated packet header including the translated packet header information in the one or more predetermined fields of the packet header interspersed with un-translated packet header information in one or more other fields of the packet header

31. (New) A bastion host as set forth in Claim 16, wherein the address includes a network portion and an apparatus portion, and wherein the bastion host is operable to translate predetermined portions of packet header information including translating the apparatus portion of the address without also translating the network portion of the address.

32. (New) A bastion host as set forth in Claim 16, wherein the data packet includes a header with a plurality of fields carrying packet header information, wherein the bastion host is operable to translate predetermined portions of packet header information including:

translating at least a portion of the packet header information in one or more predetermined fields of the header into a translated packet header, the translated packet header including the translated packet header

information in the one or more predetermined fields of the packet header interspersed with un-translated packet header information in fields other than the one or more fields of the packet header.